

Integrated Measurement and Analysis Framework (IMAF)

Chris Alberts
Julia Allen
Robert Stoddard

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon

© 2010 Carnegie Mellon University

Agenda

1. Framing the Problem Space
2. Integrated Measurement and Analysis Framework (IMAF)
3. Applying the Framework
4. Future Directions



Topic 1: *Framing the Problem Space*

1. Framing the Problem Space
 - A. Measurement Research Questions
 - B. Focus of Effective Decision Making
2. Integrated Measurement and Analysis Framework (IMAF)
3. Applying the Framework
4. Future Directions



Measurement Research Questions

- Q1: How do we establish, specify, and measure justified confidence that a software-reliant product is sufficiently secure to meet operational needs?
- Q2: How do we measure at each phase of the development or acquisition life cycle that the required/desired level of security has been achieved?
- Q3: How do we scale measurement and analysis approaches to complex environments, such as large, distributed systems of systems?



SEI Software Security Measurement Project

The focus of the project is developing an approach for providing justified confidence that a software-reliant product is sufficiently secure to meet operational needs.

- Framework
- Methods, tools, and techniques

Measurement is an essential aspect of establishing and sustaining justified confidence.

This project will develop an approach that enables decision makers to get the information they need

- When they need it
- In the format they need it



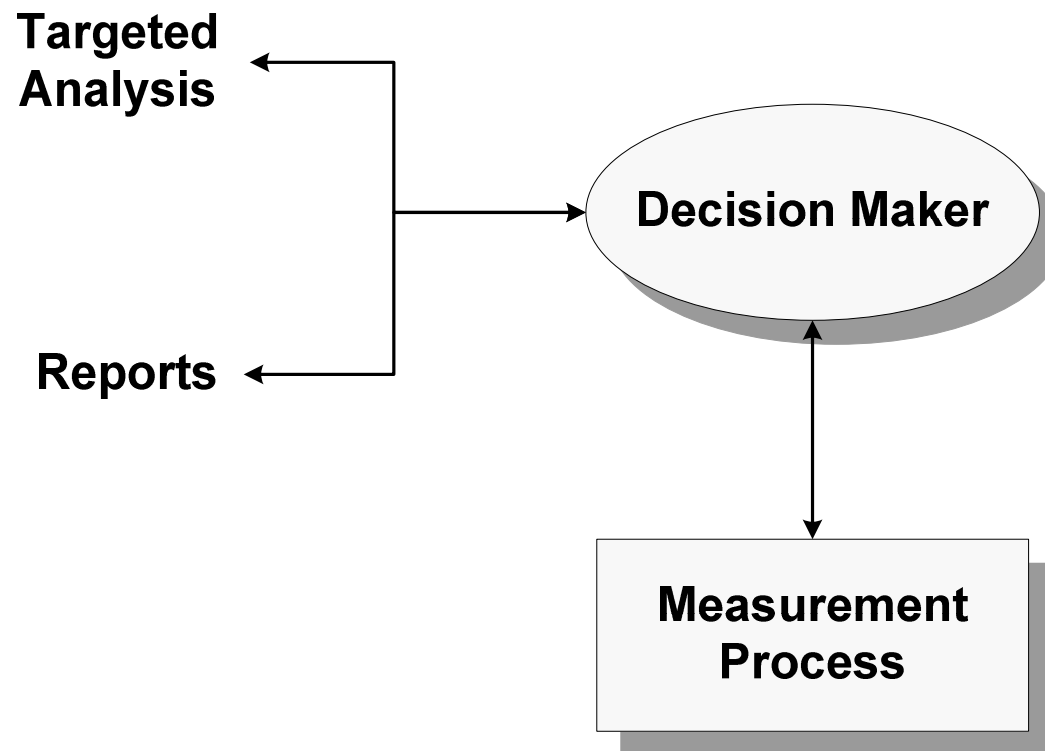
What Is Measurement?

A measurement is an observation that results in information (reduction of uncertainty) about a quantity.¹

1. Hubbard, Douglas. *Applied Information Economics Seminar: Executive Overview*. Hubbard Decision Research, 2010. <http://www.hubbardresearch.com/>



Measurement: *Focus on Effective Decision Making*



Decision makers obtain information from multiple sources, including targeted analysis (e.g., assessments), reports (verbal and written), and measurement data.



Scaling Measurement and Analysis to Complex Environments

Measurement is a well-defined discipline and has been applied successfully to software development.

However, the focus of measurement has traditionally been in the context of a single organizational entity, such as a project.

We need to find ways to scale measurement and analysis to complex environments, such as

- Acquisition programs
- Software supply chains
- Systems of systems

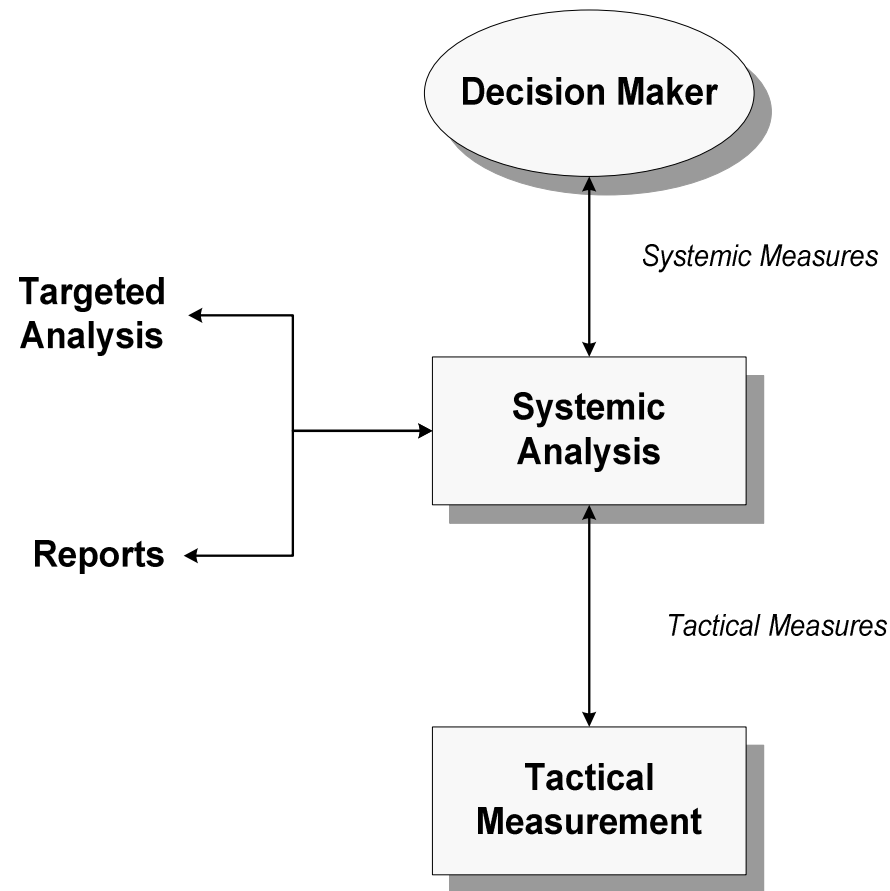


Topic 2: *Integrated Measurement and Analysis Framework (IMAF)*

1. Framing the Problem Space
2. Integrated Measurement and Analysis Framework (IMAF)
 - A. Measurement from the Systemic Perspective
 - B. Mission-Objective-Driver (MOD) Analysis
 - C. Overview of IMAF
3. Applying the Framework
4. Future Directions



Measurement from the Systemic Perspective



SEI is developing a two-tiered measurement and analysis approach for distributed management environments.



Mission-Objective-Driver (MOD) Analysis: *Implementing Systemic Analysis*

What

Mission-Objective-Driver (MOD) is a systemic approach for analyzing assurance in distributed management environments



Why

To provide an analysis approach that meets the needs of today's complex programs

Core Technologies

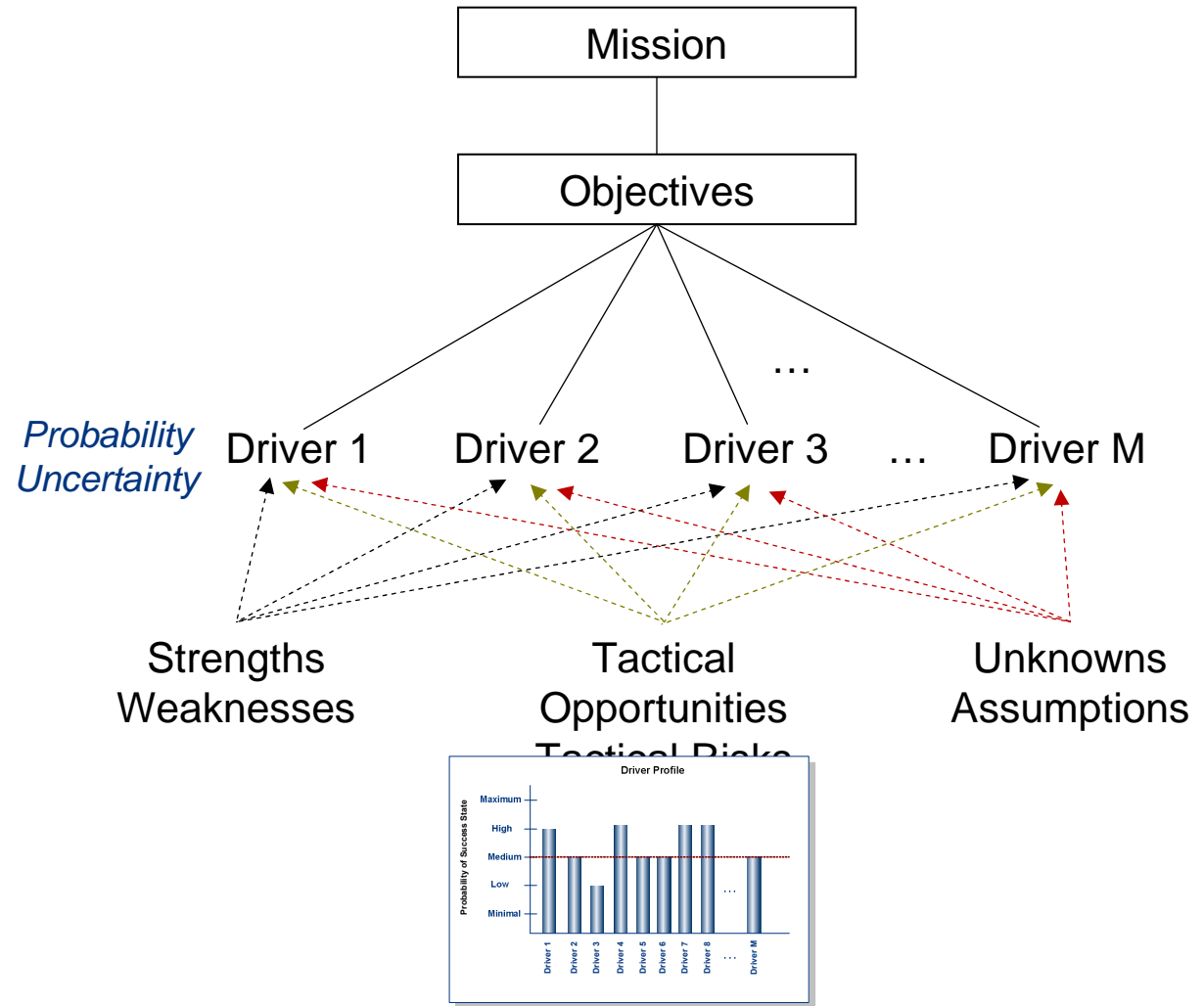
MOD Analysis Method

Driver Frameworks



MOD Analysis: *Key Activities*

1. *Document mission.*
2. *Identify objectives.*
3. *Identify drivers (i.e., factors that have a strong influence on outcome or result).*
4. *Evaluate drivers.*
5. *Document rationale and supporting data.*
6. *Establish driver profile.*



Standard Driver Framework for Software Security (Draft)

Objectives

1. Program Security Objectives

Preparation

2. Security Plan
3. Contracts
4. Security Process

Execution

5. Security Task Execution
6. Security Coordination
7. External Interfaces

Environment

8. Organizational and External Conditions

Resilience

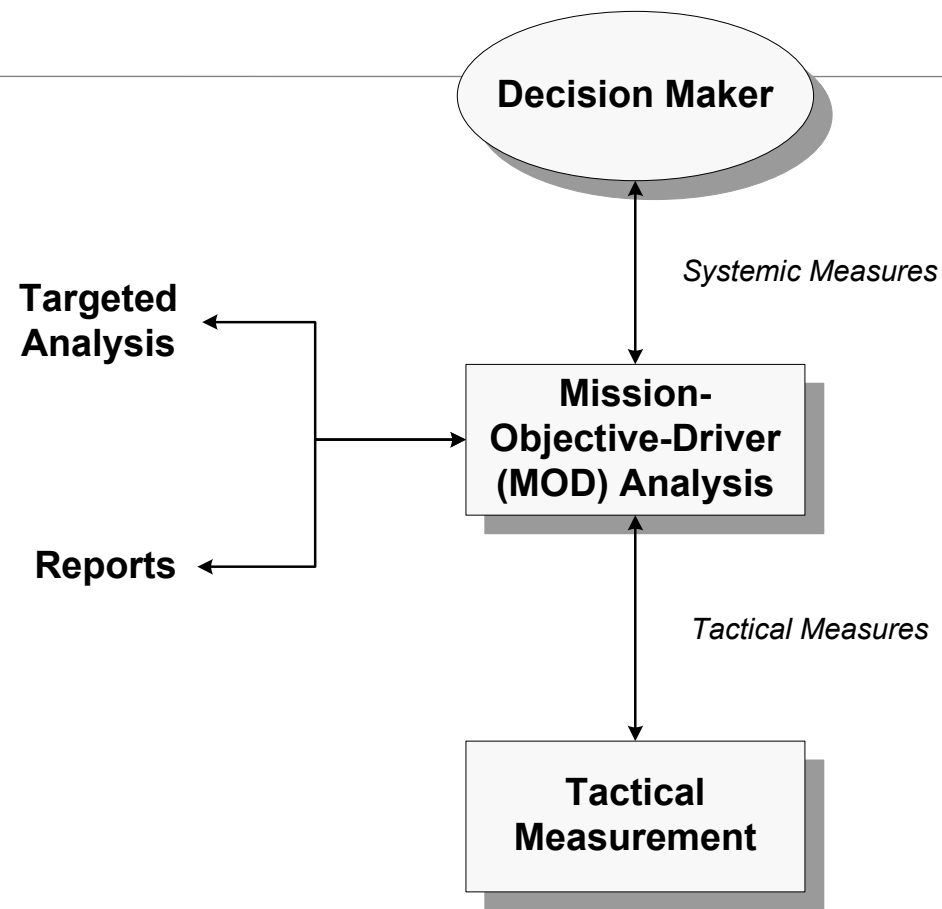
9. Event Management

Result

10. Security Requirements
11. Security Architecture and Design
12. Code Security
13. Operational System Security
14. Adoption Barriers
15. Operational Security Compliance
16. Operational Security Preparedness
17. Security Risk Tolerance



Integrated Measurement and Analysis Framework (IMAF)



Mission-Objective-Driver (MOD) Analysis links measures to the mission.

IMAF provides decision makers with insight into the mission.

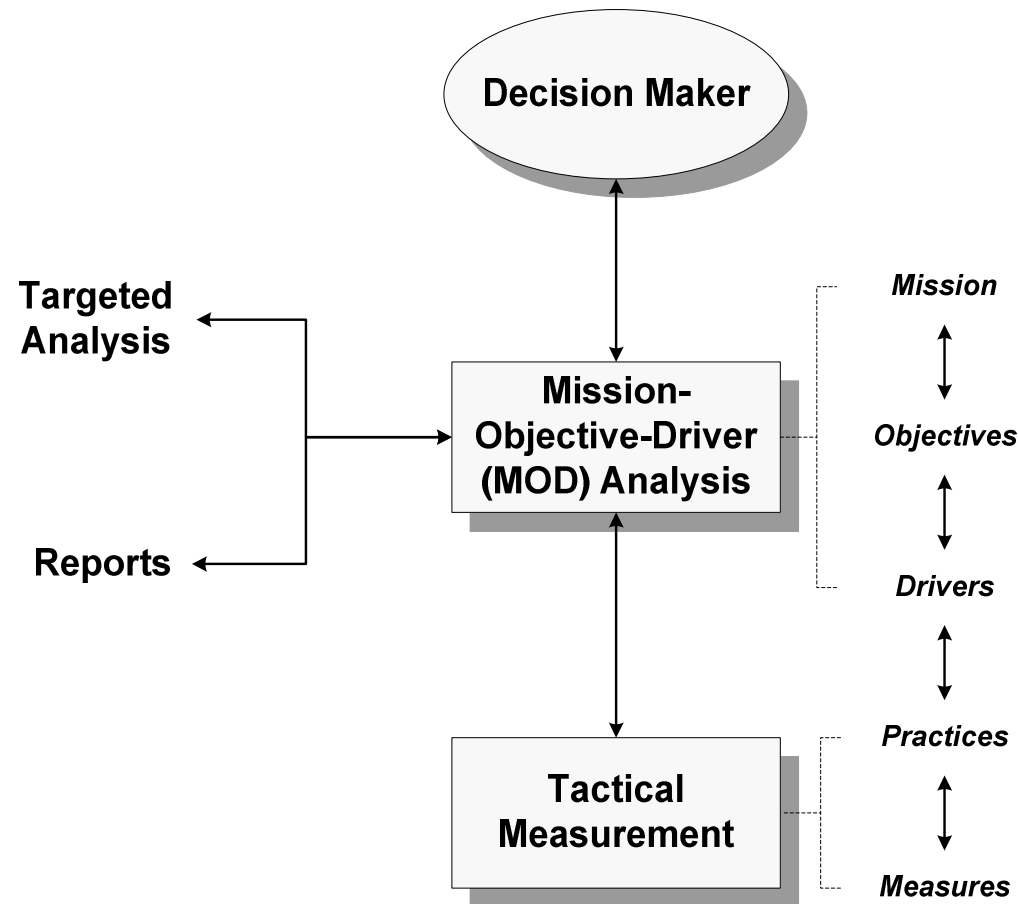


Topic 3: *Applying the Framework*

1. Framing the Problem Space
2. Integrated Measurement and Analysis Framework (IMAF)
3. **Applying the Framework**
 - A. **Aligning Drivers with Software Security Codes of Practice**
4. Future Directions



Aligning Drivers with Software Security Codes of Practice -1



IMAF provides a structure for aligning measures with the mission.



Aligning Drivers with Software Security Codes of Practice -2

For each program security driver:

1. Identify information items that are needed to address each driver
2. Determine if information items are included in one or more codes of practice
3. Build a traceability matrix of driver/practice relationships

For each selected code of practice:

1. Select a practice category or area
2. Identify information needs that practices inform
3. Determine if information needs align with one or more drivers
4. Use this analysis to suggest new drivers or lower priority practices



Example Software Security Codes of Practice

Building Security In Maturity Model (BSI-MM): <http://www.bsi-mm.com/>

Open Web Application Security Project (OWASP) Software Assurance Maturity Model:

http://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

Microsoft Secure Development Lifecycle:

<http://www.microsoft.com/security/sdl/>

Department of Homeland Security Measurement work and Assurance for CMMI Process Reference Model: <https://buildsecurityin.us-cert.gov/swa/>

CERT Resilience Management Model, Resilient Technical Solution Engineering Process Area: <http://www.cert.org/resiliency/rmm.html>



Topic 5: *Future Directions*

1. Framing the Problem Space
2. Integrated Measurement and Analysis Framework (IMAF)
3. Applying the Framework
4. **Future Directions**
 - A. **Potential Applications of IMAF**
 - B. **Discussion**



Potential Applications of IMAF

The feasibility of applying IMAF to other areas will be explored.
Candidate areas include

- Insider threat - MERIT
- Operational resilience – CERT RMM
- Others



Discussion





Software Engineering Institute

Carnegie Mellon



Software Engineering Institute

Carnegie Mellon

Integrated Measurement and Analysis Framework
© 2010 Carnegie Mellon University